UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/617,607 | 07/11/2003 | **Peng T. Ong** | AUS920085001US2 | 2901 |

50170 7590 12/07/2010

IBM CORP. (WIP)
c/o WALDER INTELLECTUAL PROPERTY LAW, P.C.
17330 PRESTON ROAD
SUITE 100B
DALLAS, TX 75252

| EXAMINER | |
|---|---|
| JOHNSON, CARLTON | |
| **ART UNIT** | **PAPER NUMBER** |
| 2436 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 12/07/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/617,607 | ONG, PENG T. | |
| | Examiner | Art Unit | |
| | CARLTON V. JOHNSON | 2436 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *06 October 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,3-7,9,10,17 and 21-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-7,9,10,17 and 21-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is in response to application amendments filed on 10-6-2010.

2. Claims **1, 3 - 7, 9, 10, 17, 21 - 31** are pending. Claims **1, 17, 28** have been amended. Claims **2, 8, 11 - 16, 18 - 20** have been cancelled. Claims **1, 17, 28** are independent. This application was filed on 7-11-2003.

### *Response to Arguments*

3. Applicant's arguments have been fully considered and were not persuasive.

3.1 Applicant argues, *in response to a coupling of a separate hardware security device to the data processing system (Remarks Page 8); from the separate hardware security device into an authentication credential container associated with the user* (Remarks Page 8)

Li discloses the viewing of authentication information such as usernames and passwords for multiple applications that are accessible by particular users. (see Li col 8, lines 4-11: GUI for system administrator to manage mail, web pages, administration duties (consolidated directory of applications); page 8, lines 31-33: rows of user information and columns of service parameters for a particular service; page 9, lines 4-14: parameters: userid, password, privileges; page 9, lines 4-20: email service configuration parameters; page 9, lines 26-31: web service configuration parameters; page 10, lines 9-12: system service configuration parameters)

In addition, Liu also discloses that input/output devices such as a transducer card reader (magnetic strip card, smart card) can be coupled to the computer system. (see Li page 21, lines 20-24: input/output devices useable by present invention include transducer card readers (magnetic strip card reader such as a smart card) This disclosure indicates that coupling to a smart card (reader) is contemplated by Li.

Deo is used to disclose a separate hardware security device (such as a smart card) which is coupled to the computing system and contains multiple applications accessible by a user. (see Deo col 2, lines 60-65: smart card (separate hardware device); each application assigned an associated certificate; col 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates or key information) Li and Deo disclose a smart card (a security device) containing multiple applications accessible by users and the capability to view authentication information for the multiple applications for particular users.

3.2 Applicant argues, *credential information comprising usernames and passwords. (Remarks Page 10)*

Deo is not used to specifically disclose authentication or credential information such as usernames and passwords. Li discloses the retrieval and viewing of usernames and password utilized to provide authentication for multiple applications accessible by users. Deo (analogous prior art) discloses a smart card which can be coupled (via a card reader) to a computing system containing authentication information. (see Li col 8, lines 4-11: GUI for system administrator to manage mail, web

pages, administration duties (consolidated directory of applications); page 8, lines 31-33: rows of user information and columns of service parameters for a particular service; page 9, lines 4-14: parameters: userid, password, privileges)

3.3 Applicant argues that the referenced prior art does not disclose, *obviousness rejection (Remarks Page 11)*

A 103 rejection based on multiple references is a legitimate technique according to the MPEP. The current application is rejected based on the Li and Deo prior art references. The set of references are in a same field of endeavor as the claimed invention, concerning the processing of authentication information for users. The 103 rejection allows portions of a claimed invention to come from different prior art references. Li discloses the processing of authentication information for multiple applications for particular users which is a concern of the claimed invention. Deo discloses the coupling of a smart card acting as a separate hardware security device containing authentication information for multiple applications for a particular user.

3.4 Applicant argues *Dependent Claims 3 - 7, 25 - 27, 29 - 31 (Remarks Page 12)*

Arguments against dependent claims 3 - 7, 25 - 27, 29 - 31 are answered by responses to independent claims 1, 17, 28. In addition, Independent claims 17 and 28 have similar limitations as independent claim 1 (Refer to Section 3.1). Responses to arguments for independent claim 1 answer arguments against independent claims 17 and 28.

3.5 Applicant argues *Claim 4 injecting authentication information. (Remarks Page 13)*

The Specification in paragraph [0048] discloses that injecting of authentication information is used during the setup of a new user to aid in the easy setup of a new user. Li discloses the setup of a new user for a computing system. For further clarity, Li also discloses the placement of default settings (authentication parameters) into a form for the new user to aid in the easy setup of a new user. (see Li page 3, Lines 9-12: default settings (parameters) are copied (injected) into a new user form for the new user. The Examiner fails to see why the copying of default settings such as authentication information into forms or templates for the new user during the setup of a new user does not satisfy the injecting limitation.

3.6 Applicant argues, *Claim 6 automatic processing of application infomration (Remarks Page 13)*

Li discloses the editing of authentication and accounting information for an application. For further clarity, LI discloses the automatic setup of services (applications) upon entering basic user information. A small subset of information is input by an administrator and the remaining configuration of the service (application) is automatically implemented and the service is available for usage by the user. (see Li page 3, lines 9-12: automatically setup and enable each service for new user)

3.7 Applicant argues, *Claim 9 injecting of authentication information (Remarks Page 14)*

Refer to Section 3.5 concerning injecting of authentication information.

3.8 Applicant argues *Claim 21 list key information (Remarks Page 14)*

Deo discloses that each application for a particular user is assigned a key. (see Deo col 2, lines 60-65: each application assigned an associated certificate (key management information such as serial number); col 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates (key management information such as a serial number); authentication information exchanged) This certificate and key information is readily available and one skilled in the art can easily incorporate this particular information within the authentication and accounting information already displayed for viewing by Li.

3.9 Applicant argues, *Claim 22 role of user (Remarks Page 14)*

Li discloses information indicating the role of a user. (see Li page 9, lines 4-14: parameters for user id, user name, privileges indicate whether user is postmaster, webmaster, administrator (role of user)) The Examiner fails to understands why the function of a user such as a webmaster, an administrator cannot be used to indicate a role of the user. Li discloses that the information associated with each application for a set of applications associated with a particular user. To one well known in the art, the role of a user is an additional parameter of information for a particular user and the addition of this piece of information to the display of application information disclosed by Li would be obvious.

3.10 Applicant argues, *Claim 25 list of personal applications accessible by user; Claims 27 delete a user name (Remarks Page 15)*

Li discloses a display of authentication information for a set of multiple applications accessible by particular users including pertinent information such as accounting information. The authentication information for multiple applications is indicated in the view or display indicated by Li. For further clarity, Li discloses the capability to delete a user name of a user from the list of applications as per claim limitation. This action will remove the particular user from accessing a particular application as per claim limitation. (see Li page 8, lines 4-11: GUI for administration; page 10, lines 29-33; page 13, lines 15-20: deleting (removing) user account information from the system)
In addition, Li also discloses the capability to edit authentication information for a particular user. (see Li page 9, Lines 8-11: agent privileges; whether or not a user is enabled (or disabled) for a particular services (application, account))

3.11 Applicant argues, *last login attempt (Remarks Page 16-17)*

Li disclose the display of authentication information for multiple applications for a particular user. Refer to Section 3.1. And, Delany discloses an indication of a last login attempt by a particular user. (see Delany paragraph [0428], lines 3-8; paragraph [0429], lines 4-7: authentication (login) attempts (successful and unsuccessful) are logged (tracked)) The logging of this accounting information makes this information readily available and one skilled in the art can easily incorporate this information within the authentication and accounting information already displayed by Li.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1, 3 - 7, 9, 10, 21 - 23, 25 - 31** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Li et al.** (Patent **WO 98/26540**) in view of **Deo et al.** (US Patent No. **5,721,781**)

**With Regards to Claim 1**, Schaeck discloses a method for providing a system administrator with a view of a totality of application accessible by a user, comprising:

b) identifying, by the data processing system, the plurality of applications accessible by the user by examining the authentication credential container associated with the user; (see Li page 8, lines 22-30: account information for services (or applications) for each user of system, information for a set of applications corresponding to a particular user)

Furthermore, Li discloses:

c) generating, by the data processing system, a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications. (see Li col 8, lines 4-11: GUI for system administrator to manage mail, web pages, administration duties (consolidated directory of applications); page 8, lines 31-33: rows of user information and columns of service parameters for a particular

service; page 9, lines 4-14: parameters: userid, password, privileges; page 9, lines 4-20: email service configuration parameters; page 9, lines 26-31: web service configuration parameters; page 10, lines 9-12: system service configuration parameters)

d) displaying, by the data processing system, the view of the administrator; (see Li col 8, lines 4-11: GUI or interface for display of information for system administrator to manage mail, web pages, administration duties, page 8, lines 31-33: user information corresponding to a particular user and service parameters for a particular service)

Furthermore, Li discloses for a): an authentication credential container associated with the user. (see Li page 8, lines 4-11: provide parameters and settings for particular services for each particular user; authentication information for a particular user) and credential information comprising user names and associated passwords for each application of the plurality of applications that the user uses. (see Li col 8, lines 4-11: GUI for system administrator to manage mail, web pages, administration duties, page 8, lines 31-33: rows of user information and columns of particulars for a particular service; page 9, lines 4-14: parameters: userid, password, privileges; page 9, lines 4-20: email service configuration parameters; page 9, lines 26-31: web service configuration parameters; page 10, lines 9-12: system service configuration parameters; the username and password parameters for a particular user associated with a particular application are indicated)

Li does not specifically disclose a separate hardware security device.

However, Deo discloses:

a) receiving, in the data processing system, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses, from the separate hardware security device; (see Deo col 2, lines 60-65: smart card (separate hardware device); each application assigned an associated certificate; col 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates or key information)

It would have been obvious to one of ordinary skill in the art to modify Li for a separate hardware security device as taught by Deo One of ordinary skill in the art would have been motivated to employ the teachings of Deo for enhanced benefits from the convenience of a smart card with multiple application after secure authentication between smart card and host systems. (Deo col 2, lines 26-29; col 2, lines 41-43)

**With Regards to Claim 3**, Li discloses the method of claims 1, further comprising removing access to an application from the plurality of the applications by utilizing the view of the plurality of the applications accessible by the user. (see Li page 8, lines 4-11: GUI administration; page 10, lines 29-33: deleting (removing) user accounting information from system; page 13, lines 15-20: deletion of user)

**With Regards to Claim 4**, Li discloses the method of claim 1, further comprising:

a) creating a user account for a new application to be accessible by the user utilizing the generated view; (see Li page 8, lines 4-11: GUI administration; page 10, lines 29-33: adding user accounting information from system; page 15, lines 15-18: add new user)

Li does not specifically disclose injecting authentication information.

However, Deo discloses:

b) injecting authentication information of the user account into the authentication credential container of the user. (see Deo col 2, lines 60-65; col 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates; authentication information transferred between smart card and host (injected or transferred between system))

It would have been obvious to one of ordinary skill in the art to modify Li for injecting authentication information as taught by Deo One of ordinary skill in the art would have been motivated to employ the teachings of Deo for enhanced benefits from the convenience of a smart card with multiple application after secure authentication between smart card and host systems. (Deo col 2, lines 26-29; col 2, lines 41-43)

**With Regards to Claim 5**, Li discloses the method of claim 4, wherein the

authentication credential container is stored at a server. (see Li page 3, lines 17-22: integrated database (storage) exists for holding settings for particular user for services available; page 21, lines 13-18: hard disks (storage))

**With Regards to Claim 6**, Li discloses the method of claim 3, wherein the removing is performed automatically. (see Li page 8, lines 4-11: GUI administration; page 10, lines 29-33: deleting (removing) user accounting information from system; page 13, lines 15-20: deletion of user)

**With Regards to Claim 7**, Li discloses the method of claim 4, wherein the creating the user account information is performed either automatically or manually by an administrator. (see Li page 8, lines 4-11: GUI administration; page 10, lines 29-33: adding user accounting information from system; page 15, lines 15-18: add new user)

**With Regards to Claim 9**, Li discloses the method of claim 4.
Li does not specifically disclose injecting authentication information.
However, Deo discloses wherein the authentication information is injected into the separate hardware security device. (see Deo col 2, lines 60-65; col 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates; authentication information transferred between smart card and host (injected or transferred between system))

It would have been obvious to one of ordinary skill in the art to modify Li for a injecting authentication information as taught by Deo One of ordinary skill in the art would have been motivated to employ the teachings of Deo for enhanced benefits from the convenience of a smart card with multiple application after secure authentication between smart card and host systems. (Deo col 2, lines 26-29; col 2, lines 41-43)

**With Regards to Claim 10**, Li discloses the method of claim 1, further comprising user directories for each application of the plurality of the applications accessible by the user. (see Li page 9, lines 26-31: indicate directory for service processing)

**With Regards to Claim 17**, Li discloses a method, in a data processing system, for providing a system administrator with a list of a plurality of applications accessible by a user together with any user names and passwords used in connection with those applications, comprising:

b) identifying, by the data processing system, the plurality of applications accessible by the user and user names and passwords used in connection with the plurality of applications by examining an authentication credential container associated with the user; (see Li page 8, lines 22-30: account information for services (or applications) for each user of system, information for a set of applications corresponding to a particular user)

c) generating, by the data processing system, a list of the plurality of applications accessible by the user together with any user names and passwords used in

connection with the plurality of applications; (see Li col 8, lines 4-11: GUI for system administrator to manage mail, web pages, administration duties, page 8, lines 31-33: rows of user information and columns of particulars for a particular service; page 9, lines 4-14: parameters: userid, password, privileges; page 9, lines 4-20: email service configuration parameters; page 9, lines 26-31: web service configuration parameters; page 10, lines 9-12: system service configuration parameters) and

d) displaying, by the data processing system. the list to the administrator. (see Li col 8, lines 4-11: GUI for system administrator to manage mail, web pages, administration duties, page 8, lines 31-33: rows of user information and columns of particulars for a particular service)

Furthermore, Li discloses for a): an authentication credential container associated with the user. (see Li page 8, lines 4-11: provide parameters and settings for particular services for each particular user)

And, Li discloses for a): credential information comprising user names and associated passwords for each application. (see Li col 8, lines 4-11: manage mail, web pages, administration duties (consolidated directory of applications); page 8, lines 31-33: rows of user information and columns of service parameters for a particular service; page 9, lines 4-14: parameters: userid, password, privileges; the username and password parameters for a particular user associated with a particular application are indicated)

Li does not specifically disclose a separate hardware security device.

However, Deo discloses:

a) receiving, in the data processing system, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device; (see Deo col 2, lines 60-65: smart card (separate hardware device); each application assigned an associated certificate; col 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates)

It would have been obvious to one of ordinary skill in the art to modify Li for a separate hardware security device as taught by Deo One of ordinary skill in the art would have been motivated to employ the teachings of Deo for enhanced benefits from the convenience of a smart card with multiple applications after secure authentication between smart card and host system. (Deo col 2, lines 26-29; col 2, lines 41-43)

**With Regards to Claim 21**, Li discloses the method of claim 1.

Li does not specifically disclose key information.

However, Deo discloses wherein the view comprises: information of keys employed by the user, wherein each entry in the list corresponds to a different key employed by the user, and wherein each entry identifies a type of the corresponding key and a serial number of the corresponding key. (see Deo col 2, lines 60-65: each application

assigned an associated certificate (key management information such as serial number); col 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates (key management information such as a serial number); authentication information exchanged)

It would have been obvious to one of ordinary skill in the art to modify Li for key information as taught by Deo. One of ordinary skill in the art would have been motivated to employ the teachings of Deo for trust between smart card and host systems from the additional security with a certificate or key based authentication system. (Deo col 2, lines 47-50)

**With Regards to Claim 22**, Li discloses the method of claim 1, wherein the view comprises: a profile of the user detailing a role of the user, a name of the user, contact information for the user, and employment information for the user. (see Li page 9, lines 4-14: parameters for user id, user name, privileges indicate whether user is postmaster, webmaster, administrator (role of user))

**With Regards to Claim 23**, Li discloses the method of claim 1, wherein the view comprises: a list of applications accessible by the user, wherein each entry in the list corresponds to a different application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding application. (see Li page 9, lines 4-14: parameters for user id, user name, privileges indicate whether user

is postmaster, webmaster, administrator (role of user))

Li does not specifically disclose a certificate-enabled application.

However, Deo discloses a certificate-enabled application. (see Deo col 2, lines 60-65: each application assigned an associated certificate; col 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates (key based authentication))

It would have been obvious to one of ordinary skill in the art to modify Li for a certificate-enabled application as taught by Deo. One of ordinary skill in the art would have been motivated to employ the teachings of Deo for trust between smart card and host systems from the additional security with a certificate or key based authentication system. (Deo col 2, lines 47-50)

**With Regards to Claim 25**, Li discloses the method of claim 1, wherein the view comprises: a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application. (see Li page 8, lines 22-30; page 8, lines 31-33: account information for each user of that system, user information corresponding to particular user and service parameters for particular service)

**With Regards to Claim 26**, Li discloses the method of claim 22, wherein the view

comprises: user selectable graphical user interface elements for invoking a function to update the profile and for invoking a function to reset the profile. (see Li page 10, lines 29-33: editing user information for system; page 13, lines 1-6: edit of user information; page 19, lines 22-24: restart newly updated account information (profile))

**With Regards to Claim 27**, Li discloses the method of claim 23, wherein the view comprises: a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of applications. (see Li page 8, lines 4-11: GUI for administration; page 10, lines 29-33: deleting users (user name))
Li does not specifically disclose a certificate-enabled application.
However, Deo discloses a certificate-enabled application. (see Deo col 2, lines 60-65: each application assigned an associated certificate; col 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates (key based authentication))

It would have been obvious to one of ordinary skill in the art to modify Li for certificate-enabled applications as taught by Deo. One of ordinary skill in the art would have been motivated to employ the teachings of Deo for trust between smart card and host systems from the additional security with a certificate or key based authentication system. (Deo col 2, lines 47-50)

**With Regards to Claim 28**, Li discloses a computer program product comprising a

computer recordable medium having a computer readable program recorded thereon, wherein the computer readable program, when executed on a data processing system, causes the data processing system to:

b) identify the plurality of applications accessible by the user by examining the authentication credential container associated with the user; (see Li page 8, lines 22-30: account information for services (or applications) for each user of system, information for a set of applications corresponding to a particular user)

c) generate a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications; (see Li col 8, lines 4-11: GUI for system administrator to manage mail, web pages, administration duties, page 8, lines 31-33: rows of user information and columns of particulars for a particular service; page 9, lines 4-14: parameters: userid, password, privileges; page 9, lines 4-20: email service configuration parameters; page 9, lines 26-31: web service configuration parameters; page 10, lines 9-12" system service configuration parameters)

d) display the view to the administrator. (see Li col 8, lines 4-11: GUI for system administrator to manage mail, web pages, administration duties, page 8, lines 31-33: rows of user information and columns of particulars for a particular service)

Furthermore, Li discloses for a): credential information for each application for an authentication credential container associated with the user. (see Li page 8, lines 4-11: provide parameters and settings for particular services for each particular user)

And, Li discloses for a): credential information comprising user names and associated passwords for each application. (see Li col 8, lines 4-11: manage mail, web pages, administration duties (consolidated directory of applications); page 8, lines 31-33: rows of user information and columns of service parameters for a particular service; page 9, lines 4-14: parameters: userid, password, privileges; the username and password parameters for a particular user associated with a particular application are indicated)

Li does not specifically disclose a separate hardware device.

However, Deo discloses:

a) receive, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications from the separate hardware security device; (see Deo col 2, lines 60-65: smart card (separate hardware device); each application assigned an associated certificate; co 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates)

It would have been obvious to one of ordinary skill in the art to modify Li for a separate hardware security device as taught by Deo. One of ordinary skill in the art would have been motivated to employ the teachings of Deo for enhanced benefits from the convenience of a smart card with multiple applications after secure authentication between smart card and host system. (Deo col 2, lines 26-29; col 2, lines 41-43)

**With Regards to Claim 29**, Li discloses the computer program product of claim 28, wherein the computer readable program further causes the data processing system to remove access to an application from the plurality of the applications by utilizing the view of the plurality of the applications accessible by the user. (see Li page 8, lines 4-11: GUI for administration; page 10, lines 29-33; page 13, lines 15-20: deleting user information (remove access for a user))

**With Regards to Claim 30**, Li discloses the computer program product of claim 28, wherein the computer readable program further causes the data processing system to:

a) create a user account for a new application to be accessible by the user utilizing the generated view; (see Li page 8, lines 4-11: GUI for administration; page 10, lines 29-33: adding a new user)

Li does not specifically disclose inject authentication information.

However, Deo discloses:

b) inject authentication information of the user account into the authentication credential container of the user. (see Deo col 2, lines 60-65: each application assigned an associated certificate; col 3, lines 10-15; col 3, lines 18-23: smart card and terminal verify authenticity of each other, application is selected, smart card and terminal then authenticate application using exchanged certificates; authentication information transferred between smart card and host (injected or transferred between system))

It would have been obvious to one of ordinary skill in the art to modify Li for injecting authentication information as taught by Deo One of ordinary skill in the art would have been motivated to employ the teachings of Deo for enhanced benefits from the convenience of a multiple application smart card with multiple applications after secure authentication between smart card and host system. (Deo col 2, lines 47-50)

**With Regards to Claim 31**, Li discloses the computer program product of claim 28, wherein the view comprises the following:

d) user selectable graphical user interface elements for invoking a function to update the profile and for invoking a function to reset the profile; (see Li page 8, lines 4-11: GUI for administration; page 10, lines 29-33; page 13, lines 1-6: editing user account information of the system)

e) a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of certificate-enabled applications; (see Li page 8, lines 4-11: GUI for administration; page 10, lines 29-33; page 13, lines 15-20: deleting (removing) user account information from the system)

Deo discloses a certificate-enable application as disclosed in Claim

and the following non-selected views:

a) a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled application, and wherein each entry identifies a user name of the user and a last login attempt of

the user for the corresponding certificate-enabled application; and b) a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application; c) a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application.

5. Claim **24** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Li et al.** (Patent **WO 98/26540**) in view of **Delany et al.** (US PGPUB No. **20020138763**)

**With Regards to Claim 24**, Li discloses the method of claim 1, wherein the view comprises: a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user for the corresponding enterprise application. (see Li page 9, lines 4-14: parameters for user id, user name, privileges indicate role of user)
Li-Deo does not specifically disclose tracking a last login attempt.
However, Delany discloses wherein a last login attempt of the user for corresponding entries application. (see Delany paragraph [0428], lines 3-8; paragraph [0429], lines 4-7: authentication (login) attempts (successful and unsuccessful) are logged (tracked))

It would have been obvious to one of ordinary skill in the art to have modified Li-

Deo for last login attempt as taught by Delany. One of ordinary skill in the art would have been motivated to employ the teachings of Delany to the convenience of addition and removal of user accounting and authentication attributes for an existing group using a centralized source. (see Delany paragraph [0014], lines 4-7; paragraph [0014], lines 10-14)

## *Conclusion*

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
November 22, 2010

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436